SYSTEM AND METHOD FOR PRESORTING RULES FOR FILTERING PACKETS ON A NETWORK

FIELD AND BACKGROUND OF THE INVENTION

The present invention relates to a system and method for presorting rules for filtering packets on a network, and in particular for presorting such rules according a user profile.

Security of information is extremely important for modern society, particularly since the advent of the Internet. Unauthorized exposure of such information, and/or unintended or unauthorized use of information may significantly damage organizations and individuals. Damage may also be caused by lost, corrupted or misused information. Thus, appropriate security measures are required in order to protect information from such damaging actions, while still maintaining the availability of such information to authorized individuals and/or organizations.

Currently, flexibility and ease of access to information are highly valued, particularly through the Internet and organizational intranets, which provide connections between computers through a network. Accessing information through a network enables users at physically separate locations to share information, but also increases the possibility of unauthorized or unintended access to the information. Various attempts to provide a solution to the problem of security for electronically stored information are known in the art, but all of these attempted solutions have various drawbacks.

For example, a "firewall" is a software program or hardware device which attempts to provide security to an entire network, or to a portion thereof, by filtering all communication which passes through an entry point to the entire network or the portion of the network. The filtration of packets is performed according to one or more rules, such that if the packet does not conform to these rules, then the packet is blocked from entry to the entry point. An example of such a firewall is disclosed in U.S. Patent No. 5,606,668, incorporated by reference as if fully set forth herein.

Unfortunately, currently available firewalls have a number of disadvantages. In particular, these firewalls can be extremely slow and non-selective in terms of the application of the rules. For example, U.S. Patent No. 5,606,668 neither teaches nor suggests a step of presorting the rules according to a characteristic of the packet. Such presorting could significantly reduce the number of rules which would need to be examined in reference to the

packet, and hence would greatly increase the speed of filtering packets. Unfortunately, a firewall with such presorting is not currently available.

There is thus a need for, and it would be useful to have, a system and a method for presorting rules for application to a packet as part of a network security filter according to a characteristic of the packet, and preferably according to at least one of the source address and destination address, thereby reducing the number of rules which must be applied to the packet in order to increase the rate of filtering.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, wherein:

FIG. 1 is a schematic block diagram of a system according to the present invention; and

FIG. 2 is a flowchart of a method according to the present invention.

SUMMARY OF THE INVENTION

The present invention is of a method and a system for presorting rules for filtering a packet in a network security filter according to a characteristic of the packet, preferably at least one of the source address and destination address. The advantage of presorting rules before application to the packet is that the number of rules which must be examined should be significantly reduced. In addition, the source address and/or destination address can be associated with a particular profile, which may be associated with a particular user for example. The rules are also more easily managed according to such profiles, since the network manager or system administrator can choose a set of rules for the profile, and then amend the profile as a whole, rather than attempting to apply disparate, unrelated rules for filtering. Thus, the method and system of the present invention are more efficient both for actual filtering of packets, and for management of the security network filter.

According to the present invention, there is provided a method for presorting a plurality of rules for filtering a packet in network, the method comprising the steps of: (a) selecting a characteristic for sorting the plurality of rules, the characteristic having a plurality of possible values; (b) associating each rule with at least one value for the characteristic; (c) receiving the packet; (d) at least partially analyzing information in the packet to obtain the value for the characteristic; (e) selecting at least one of the plurality of rules according to the value to form at

least one selected rule; and (f) applying the selected rule to the packet, such that the packet is permitted to enter the network or alternatively is dropped.

Hereinafter, the term "network" refers to a connection between any two electronic devices which permits the transmission of data.

Hereinafter, the term "security network filter" also refers to firewalls and any other type of mechanism for filtering packets according to one or more rules.

Hereinafter, the term "wireless device" refers to any type of electronic device which permits data transmission through a wireless channel, for example through transmission of radio waves. Hereinafter, the term "cellular phone" is a wireless device designed for the transmission of voice data and/or other data, through a connection to the PSTN (public switched telephone network) system.

Hereinafter, the term "computer" includes, but is not limited to, personal computers (PC) having an operating system such as DOS, Windows™, OS/2™ or Linux; Macintosh™ computers; computers having JAVA™-OS as the operating system; and graphical workstations such as the computers of Sun Microsystems™ and Silicon Graphics™, and other computers having some version of the UNIX operating system such as AIX™ or SOLARIS™ of Sun Microsystems™; or any other known and available operating system. Hereinafter, the term "Windows™" includes but is not limited to Windows95™, Windows 3.x™ in which "x" is an integer such as "1", Windows NT™, Windows98™, Windows CE™ and any upgraded versions of these operating systems by Microsoft Corp. (USA).

The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware or firmware, or a combination thereof. For the present invention, a software application could be written in substantially any suitable programming language, which could easily be selected by one of ordinary skill in the art. The programming language chosen should be compatible with the computer hardware and operating system according to which the software application is executed. Examples of suitable programming languages include, but are not limited to, C, C++ and Java.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is of a method and a system for presorting rules for filtering a packet in a network security filter according to a characteristic of the packet. The characteristic is preferably at least one of the source address and destination address. The advantage of

presorting rules before application to the packet is that the number of rules which must be examined should be significantly reduced. Furthermore, those rules which are selected after the presorting procedure for application to the packet are therefore more relevant to that particular packet, such that the analysis of the packet is more efficient.

In addition, the source address and/or destination address can be associated with a particular profile, which may be associated with a particular user for example. The rules are also more easily managed according to such profiles, since the network manager or system administrator can choose a set of rules for the profile, and then amend the profile as a whole, rather than attempting to apply disparate, unrelated rules for filtering. For example, different levels of user permissions may be determined according to company policy, such that a basic profile for each level of permission would be provided. The system administrator or network manager would therefore select the profile, which would already contain all of the necessary general rules. Optionally, if necessary, one or more changes to the rules could be made in order to fully optimize the rules for the particular source and/or destination address for that user. Thus, the method and system of the present invention are more efficient both for actual filtering of packets, and for management of the security network filter.

The principles and operation of a system and a method according to the present invention may be better understood with reference to the drawings and the accompanying description, it being understood that these drawings are given for illustrative purposes only and are not meant to be limiting.

Referring now to the drawings, Figure 1 is a schematic block diagram of an exemplary system **10** according to the present invention for filtering packets according to a plurality of presorted rules. System **10** features a network **12** with an entry point **14**, which is preferably a computer connected to network **12**. Preferably, all network traffic must pass through entry point **14** for transmission on network **12**, although a plurality of such entry points **14** may optionally be present on network **12** (not shown). Network **12** also features a plurality of endpoint computers **16** for transmitting and receiving packets. Each such endpoint computer **16** features an address, such that each packet has a source address, which may be from an endpoint computer **16** within network **12** or from a network entity outside network **12**, and a destination address, which is within network **12**. In the simplified network shown, the destination address would be for an endpoint computer **16**. It is understood that the structure of network **12** has been simplified for the sake of clarity, and is not meant to be limiting in any way. Furthermore, techniques for

constructing various configurations of networks are well known to those of ordinary skill in the art. The present invention is operative with any possible network configuration.

A network security filter **18** is installed at entry point **14**. As described previously, network security filter **18** may be implemented as software, hardware, firmware or a combination thereof. Network security filter **18** must have access to packets being transmitted through entry point **14**. Network security filter **18** then first retrieves at least one characteristic of the packet, which is preferably at least one of a source address and a destination address of the packet, and uses this characteristic to presort a plurality of filtering rules which are stored in a rules database **20**. Only those rules which are indicated as being relevant for that value of the characteristic, such as a particular source address or destination address, or combination thereof, are then applied to the packet by network security filter **18**. The process of applying the rules involves further analysis of the packet to obtain the necessary information, and then comparing the information in the packet to the rule, such that if the rule is not fulfilled, the packet is rejected or dropped. The dropped packet cannot then enter network **12** through entry point **14**. Optionally and additionally, an alarm or other indication is given, and/or an entry is made in a log file, if one or more rules are violated by the packet.

Preferably, the rules contained in rules database **20** are presorted according to a plurality of possible values for the characteristic which is examined, more preferably with a default value. Therefore, when the characteristic of the packet is analyzed and the value is retrieved, network security filter **18** is able to quickly retrieve only those rules from rules database **20**. Alternatively, the rules may not be presorted, but may instead be sorted separately for each incoming packet by network security filter **18**.

As previously described, and as described in greater detail below with regard to Figure 2, the characteristic which is preferably retrieved from the packet in order to sort the rules is at least one of the source address and the destination address of the packet. The source address and/or the destination address may be associated with a particular user, such that the permissions and restrictions placed upon the behavior of the user within network **12** are reflected in terms of the rules applied to packets associated with that user. Using the source address and/or the destination address as the characteristic for sorting the rules has the advantage that users who are located at computers outside of network **12** (not shown) may be accorded certain privileges for entry through entry point **14**. Thus, a user who is working at home, while traveling, or at a remote office, for example, may be granted certain privileges in terms of the permitted behavior of the packet.

With regard to the actual application of the rules to the packets, as well as of the construction of the rules themselves, these aspects of filtering the packets are known in the background art. In particular, these functions are described in U.S. Patent No. 5,606,668, previously incorporated by reference. Briefly, a packet enters entry point **14** and passes through layers 1 and 2 of the ISO (International Standardization Organization) model of communication protocol layers for a network. The packet is then diverted to network security filter **18**. Network security filter **18** then analyzes information contained within the packet, which may for example optionally include information in one of the headers or alternatively the data being carried by the packet. Preferably, the packet is analyzed from the uppermost header, which is the IP (Internet Protocol) header, to the data being carried, such that each layer of information is retrieved from the packet and compared to one or more rules. If at least one rule is violated, then either network security filter **18** drops the packet, or at least indicates the presence of a rules violation. If network security filter **18** determines that a terminal violation has occurred, such that the packet is forbidden to enter network **12** because of the particular violation, the analysis is preferably stopped and the packet is dropped.

Figure 2 is a flowchart of an exemplary method for preparing a user profile, and for then applying the presorted rules to a received packet. In step 1, the characteristic for sorting the rules is selected. Preferably, the characteristic is at least one of the source address of the packet and the destination address of the packet, and is more preferably a combination thereof. In step 2, a plurality of rules are constructed. For example, a rule may be simple, such that no incoming connections to a particular port associated with a particular service are permitted. Optionally, a rule may be complex, involving a variety of factors such as the source address of the packet, the type of application generating the data contained in the packet and so forth. In step 3, optionally users who are associated with a value for the characteristic are given a particular level of permissions and privileges, which then constitute the user profile. For example, users at a certain level may not have permission to receive HTML (HyperText Mark-up Language) documents, such that they cannot download Web pages.

In step 4, each rule is associated with at least one value for the selected characteristic, and preferably is associated with a plurality of such values. For example, each rule may be associated with at least one source address, or a class of such source addresses which may be defined by grouping the users associated with those addresses into certain levels of permissions, as previously described. If a user profile is available, preferably the restrictions and privileges contained therein are used to associate each rule with one or more values for the selected

characteristic. In step 5, optionally and preferably, the rules are presorted according to the associated value or values for the selected characteristic, in order to facilitate later application of the rule to information contained in the packet.

In step 6, a packet is received by the network security filter. In step 7, the information contained in the packet is at least partially analyzed in order to obtain the value for each characteristic which is used to sort the rules. As previously described, this characteristic is preferably at least one of the source address and destination address. In step 8, the value or values are used to selected the rule(s) which are to be applied. In step 9, the rules are applied, such that the packet is either permitted to enter the network or is dropped.

It will be appreciated that the above descriptions are intended only to serve as examples, and that many other embodiments are possible within the spirit and the scope of the present invention.